IN THE CLAIMS:

Claims 1-19 (Cancelled)

20. (Previously Presented) A method, comprising:

enabling integrity checking of a software module to be used in a mobile communication terminal, said terminal communicating in a mobile communication system, said software module already stored on a removable memory unit connected to the terminal and ready for use except, before allowing the software module to take control of the terminal, the terminal communicates via the mobile communication system with a software provider, said terminal comprising a processor configured to carry out said enabling by:

hashing the software module on the removable memory unit, resulting in a first hash value,

transmitting by said terminal of identifying information concerning said terminal and said memory unit to said software provider, wherein said transmitting of identifying information comprises transmitting a first identifier, associated with the memory unit, a second identifier, associated with the terminal and the first hash value via the mobile communication system to said software provider,

receiving by said terminal from said software provider a digitally signed data block comprising a reference value for use during integrity checking of said software module, said data block comprising a digital signature and further data associated with the memory unit and the terminal,

analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers,

if the comparison of said further data matches with said first and second identifiers, storing the received data block comprising the digital signature, thereby providing the reference value for use during integrity checking of said software module; and

wherein said integrity checking further comprises hashing the software module for providing a second hash value using the reference value, and checking whether or not the second hash value matches the first hash value and if the second hash value matches the first hash value allowing the software module to run on and take control of the mobile communication terminal.

21. (Cancelled)

22. (Currently Amended) An apparatus, comprising:

a processor for enabling integrity checking of a software module to be used in said apparatus, said apparatus for communicating in a mobile communication system, said software module already stored on a removable memory unit for connection to the apparatus and ready for use after said connection except, before allowing the software module to take control of the apparatus, the ~~terminal~~apparatus communicates via the mobile communication system with a software provider, wherein said processor, in enabling said integrity checking ~~a device for hashing~~hashes the software module, resulting in a first hash value;

a transmitter for transmitting identifying information concerning said apparatus and said memory unit to said software provider wherein transmittal of said identifying information comprises transmittal of a first identifier associated with the memory unit, a second identifier associated with the apparatus and the first hash value via the mobile communication system to said software provider;

a receiver for receiving, from the software provider, a data block comprising a digital signature and further data associated with the memory unit and the ~~terminal~~apparatus;

said processor for analyzing the received data block, comprising verification of the digital signature and comparison of said further data with said first and second identifiers;

a memory device for storing the received data block comprising the digital signature, thereby providing a reference value for use during integrity checking of said software module for a receiver for receiving a digitally signed data block comprising ~~a~~ the reference value for use during integrity checking of said software module; and

wherein said integrity checking comprises hashing the software module for providing a second hash value, and checking whether or not the second hash value matches the first hash value and if the second hash value matches the first hash value allowing the software module to run on and take control of the apparatus.

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)